U.S. Department of Education
Federal Student Aid

Production Readiness Review (PRR)
Process Description

Version 8.1

Final

January 30, 2009

Document Version Control

Version	Date	Description
8.1	01/30/2009	• Modified Applicability section to address concerns related conducting PRRs on infrastructure and toolset changes. • Clarified the sign-off authorities for the CIO signature line. • Added Checklist items to cover re-validation of disaster recovery objectives (RTO and RPO) and vulnerability scans. • Minor clarifications in PRR checklist definitions.
8.0	7/30/2008	Major Document Revision includes the following: • Major Checklist updates to reflect stakeholder discussions • New information regarding rationale for holding PRRs • New diagram depicting the role of the PRR in the context of other related activities • Addition of PRR presentation slides • Updated signoff role descriptions • Updates to signature page • Updated terminology based on VDC Configuration Management Database (CMDB) Data Dictionary, ECOM, and Security documents. • Major formatting and editorial changes to conform to the Federal Student Aid Document Template
1.0 - 7.0	6/19/2007	For previous revision history of Versions 1.0-7.0, see Version 7.0

TABLE OF CONTENTS

SECTION 1. LEGISLATIVE BACKGROUND

The Production Readiness Review (PRR) Process is a process that has been put in place by Federal Student Aid to reduce the likelihood of new releases causing unintended adverse impact to end-users. This process also supports the responsibilities of Federal Student Aid's Chief Information Officer (CIO), as described by the Clinger-Cohen Act. These include:

- Developing, maintaining, and facilitating the implementation of sound and integrated information technology architecture.

- Promoting the effective and efficient design and operation of all major information resource management processes.

SECTION 2. PURPOSE

The purpose of the PRR is to establish a common process that defines the activities and the roles of all groups supporting the government's decision to implement a new information system or a new release of an existing system. The PRR serves as the final, formal, and documented decision point before a new system or a significant release of an existing system enters Federal Student Aid's production environment and is exposed to end-users.

Completion of a PRR accomplishes the following:

- Demonstrates to Federal Student Aid's senior management the readiness of the system to enter production.

- Reviews the testing approach, participation, and test results to ensure that the system has been adequately tested and is ready for use by end-users.

- Discloses areas of risk associated with the system moving into production and the associated risk mitigation strategies. This ensures that Federal Student Aid Management is aware of all risks associated with a release and has accepted the risk of implementing the system. For systems where users are Trading Partners, Students, Parents, or Borrowers, completion of a PRR acknowledges that Federal Student Aid management has accepted the risks associated with public exposure of the system.

- Reviews Lessons Learned and Process Improvements.

- Acquires formal authorization to move the system into production as indicated by completion of a PRR Sign-Off Memorandum (Appendix D).

SECTION 3. APPLICABILITY

The PRR Process applies to initial releases of applications entering Federal Student Aid's Data Center Production Environment. The PRR Process also applies to significant enhancements to existing applications. An application consists of business logic that directly impacts end-users (students, parents, schools, financial aid administrators, borrowers, lenders, guarantee agencies, government employees and contractors).

The PRR Process is not required for releases that are solely related to the deployment of infrastructure (e.g. changing a router). The PRR Process is also optional for emergency releases, operating system upgrades and patches (including midrange and mainframe operating system upgrades), upgrades and patches to commercial-off-the-shelf software (COTS) that do not impact end users, and build-out of tool sets within the operating environment.

While the PRR Process is optional for infrastructure and tool sets when they are initially deployed, these items are a critical component of supporting applications in the operating environment and must be taken into consideration when an application team performs a PRR.

General Guide for PRR Applicability	
Release Description	PRR Required or Optional
Applications (initial releases and significant enhancements) – Includes all business logic that impacts end users.	Required
Infrastructure – Includes all hardware and operating system components.	Optional
Significant COTS releases that impact end users	Required
COTS Upgrades and Patches that do not impact end users	Optional
COTS-based Tool Sets – Releases that deploy tool sets into the operating environment and do not impact end users.	Optional
Re-design of websites	Required
Minor content updates to websites	Optional

Federal Student Aid's Chief Operating Officer (COO), Chief Information Officer (CIO), or the Virtual Data Center (VDC) Manager may request that a PRR be completed for any release. If the Application Owner disagrees with this request, the application may not enter the production environment until FSA's CIO and other members of the leadership team have made a determination.

If project teams have questions related to the applicability of PRR to a particular release, those questions should be resolved at the weekly VDC Projects and Operations Meeting or by coordinating with the CIO Enterprise Quality Assurance Team.

SECTION 4. PRR PROCESS STEPS

Step 1: Preparation

The project team prepares for a PRR by reviewing and preparing internal documentation and reviewing the status of the system. The team also prepares a briefing and sign-off memorandum for the formal PRR presentation. To ensure that all documents are ready for the formal PRR and there are no outstanding issues that need to be resolved prior to the PRR, it is strongly recommended that large systems or releases hold a "pre-PRR" with the project team, the Independent Verification & Validation (IV&V) contractor, and security certification and accreditation (C&A) team. A critical component of the PRR is the PRR Summary Checklist (Appendix B) for use in performing a gap analysis. The gap analysis provides the basis for the risk identification and the development of the risk mitigation strategy. Appendix C provides a guide for the checklist including each section's point of contact (POC) and checklist definitions (Appendix C).

Step 2: Collaboration

The project team should collaborate with other areas of Federal Student Aid that support the system release to implement the following functions:

- Identify all external organizations and representatives who will participate in the PRR process, including the VDC Manager, other impacted systems (if any), security staff, the CIO Enterprise Quality Assurance (EQA) Team, and others as appropriate.

- Coordinate with the EOCM process, as required, for all enterprise events associated with any operational system or system component. The EOCM process will be used for all enterprise events associated with any operational system or system component. An enterprise event is a change that impacts Federal Student Aid across multiple systems or interfaces, including changes to enterprise architecture components and Federal Student Aid-wide business requirements. Reference: EOCM Plan, Version 1.1 (November 7, 2007).

- Initiate discussions with each external organization and representative to identify their individual needs and requirements; a joint PRR may be appropriate for releases where multiple systems are implementing related changes.

- Design a comprehensive Gap Analysis, which identifies all incomplete activities from the Appendix B – Summary Checklist, the assessment of risk associated with the gap, and the time and schedule implications associated with eliminating the gap. There is a cost-benefit factor to the elimination of gaps that should be considered. (Not all gaps need to be eliminated, but Federal Student Aid approval is required with an action plan provided to close the gap.)

- Prepare a risk analysis and risk mitigation strategy for outstanding risks.

- Discuss the PRR presentation outline with the Technical Lead, Application Owner, and CIO contacts prior to the formal presentation to address specific concerns that senior managers may have with the release.

Step 3: Presentation and Sign-Off

A PRR meeting must be held to provide a forum for formal discussion and approval of the release moving to the production environment. The Federal Student Aid Technical Lead is responsible for directing the preparation of the presentation and selecting the appropriate presenter(s). The presentation is delivered by the Technical Lead to the Application Owner / Business Owner and Federal Student Aid's CIO. The presentation should not exceed one hour in length, including questions and answers. The presentation is an executive overview of the production readiness of the system release. Detailed supporting documentation, including but not limited to a completed PRR checklist (Appendix B), must be available at the PRR meeting to back up any claims, assertions, or metrics presented and will be made available to all attendees at the start of the presentation.

The PRR is a critical meeting that is the final decision point in the development process before implementation begins. The following diagram displays the PRR meeting in the context of other critical activities related to the implementation release schedule.
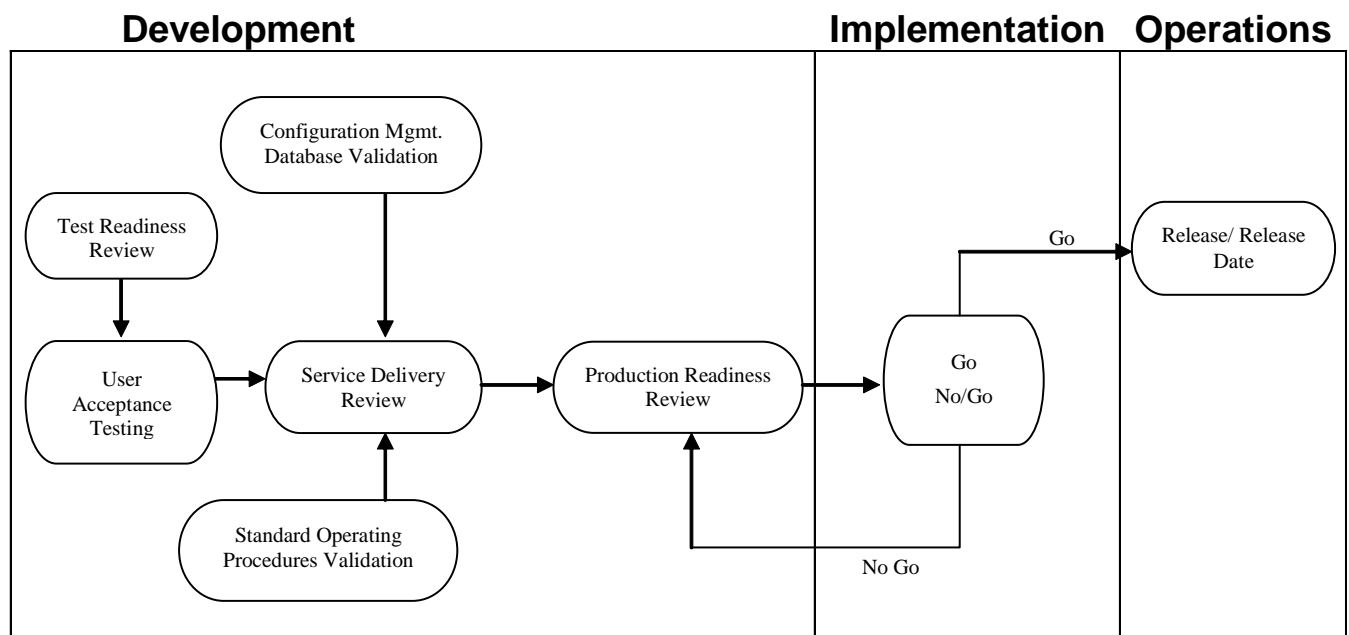

Figure 1, Role of PRR Process

SECTION 5. PRR PRESENTATION OUTLINE

The presentation outline may be customized to meet the needs and interests of the application owner and Federal Student Aid's CIO; however, all information included in the outline below must be covered, in some form, during the presentation. Additional information and issues may be included in the PRR presentation, as necessary.

Section 1: Business Background

- Business drivers for the release
- Expected Business Benefits

Section 2: Schedule

- Planned Development Schedule (Baseline)
- Actual Schedule
- Schedule information must specifically show the time that was allotted for testing activities.

Section 3: Testing Summary

- High Level Test Summary. This includes the types of tests conducted (Integration, System, Inter-system Testing, User Acceptance Testing, 508 Accessibility Testing, Performance and Capacity Testing, and Security) including high level issues found by each phase of testing that is performed for the particular project.
- Incident Report by Testing Phase. This slide includes total number of defects identified by criticality (Urgent, High, Medium and Low) within each type of testing and categorized by the statuses of Open, Closed, Deferred and Enhancements.

Section 4: Collaboration and Coordination

- Appropriate Security Reviews have occurred (C&A complete, if applicable)
- Disaster Recovery Objectives have been communicated
- VDC Readiness - Responsibility, Accountability, Counsel, Informed (RACI)
- Operations Maintenance Readiness
- Service Desk Readiness
- Training
- EOCM Related Activities

Section 5: Independent Verification & Validation (IV&V), if applicable

- Summary of approach, activities, and results.

- IV&V Recommendation (Go, Go with Reservations (list reservations), No Go); IV&V's recommendation is based on all requirements being implemented and tested and there being no critical defects. IV&V will notify the application owner and EQA prior to the PRR if a recommendation is conditional or a "No Go." See the Federal Student Aid IV&V Handbook for more details on IV&V's role in the PRR process. If a No Go decision is reached, no signatures are obtained and key action items required to be met must be documented. Once the action items are addressed, another PRR presentation is required and will be held prior to implementation approval being given.

Section 6: Risk Summary

- Risks and mitigation strategies

- Outstanding Issues/Action Items

- Specific identification of known risks that are being accepted with the decision to implement the release

Section 7: Lessons Learned

- General Lessons Learned

- Project-Specific Lessons Learned

Section 8: Meeting Closure

- Completion of formal sign-off memorandum

- Delivery of sign-off memorandum and supporting documentation to CIO EQA Team (may be completed after meeting)

SECTION 6. SIGN-OFF

The primary output of the PRR Meeting is a memorandum that formally authorizes a system or release to move into the production environment. A sample sign-off memorandum is presented in Appendix D. The sign-off memorandum may be tailored to the needs of the project, subject to the following conditions:

1. Only government employees may sign the memorandum (contractors may not sign). A PRR represents the government's decision to implement a release and the government's acceptance of risk associated with that implementation. It is suggested that government staff obtain a separate memorandum from contractors recommending Go or No/Go at a PRR, but the final decision to implement (or not to implement) a release must be made by government staff.

2. The following are the minimum signatures required for sign-off:

   - System Technical Lead

   - System Security Officer (SSO)

   - VDC Manager

   - Enterprise Quality Assurance

   - CIO*

   - Application Owner

In the event sign-off does not occur, concurrence should be reached on the actions, activities, or deliverables that must be completed prior to implementation.

At the discretion of the Application Owner and the CIO, sign-off may occur provided these agreed upon provisions are met, or another presentation and production readiness meeting may be required.

There are four potential outcomes of the sign-off:

   - **Unconditional Sign-off -** indicates that all required signatures are obtained at the production readiness review meeting and there are no outstanding issues that must be resolved prior to implementation.

   - **Conditional Sign-off -** indicates that although all required signatures are obtained, implementation may not occur until certain conditions are met. These conditions should be written on the front of the memorandum before it is signed, or on the back of the memorandum with a notation on the front that the approval is conditional. The technical lead for the release is responsible for ensuring that all the identified conditions are met before the release is moved to the production environment. An additional PRR meeting is not required.

   - **Provisional Sign-off -** indicates that one or more signatures were NOT obtained. Conditions have been identified that must be met before the missing signatures can be

obtained. Once the conditions are met, the signatures can be obtained individually; an additional PRR meeting is not required, but may be requested by any of the signatories.

- **No Sign-off -** indicates that insufficient information exists at this time to approve the system for production and/or the project is not ready to be implemented. In this case, no signatures are obtained and key action items required to be met must be documented. The missing information should be clearly identified and understood so that the next PRR will be successful. Once those actions are met, another PRR presentation is required and will be held prior to implementation approval being given.

* The CIO has delegated sign-off responsibilities for PRR, depending on the size, scope, and complexity of the release. The CIO Enterprise Quality Assurance Team will make a risk-based determination and coordinate for the appropriate CIO representative to be present at each PRR based on the following guidelines:

- Initial releases of major applications and system integration projects require the signature of the CIO. In general, these releases have a significant impact on the way that FSA does business and/or interacts with a substantial end-user population.
- Significant updates to major applications, initial releases of non-major applications, and large-scale annual releases may be signed by one of the three CIO Directors.
- Mid-size changes to application business logic that are routine in nature, releases where the only end-users are government employees or contractors, and releases that pose a low risk Federal Student Aid's core business may be signed by the VDC Manager or Enterprise Quality Assurance Program Manager.

SECTION 7. SIGN-OFF RESPONSIBILITIES

Technical Lead/System Manager - The Technical Lead/System Manager's signature certifies that all reasonable due diligence has been exercised to assure system stability/operability, that known risks have been identified/described in the presentation, and that testing has been performed, with the results indicating that a business benefit will be derived by the implementation of the system.

Information System Security Officer - The Information System Security Officer's signature certifies that all reasonable due diligence has been exercised to assure system security, and known risks have been identified/described in the presentation and in the supporting documentation.

Government VDC Manager - The Government VDC Manager's signature certifies that all VDC issues and concerns have been addressed and the VDC is ready to accept the system into the production environment.

Enterprise Quality Assurance Program Manager - The Enterprise Quality Assurance Program Manager's signature certifies that the PRR was conducted in accordance with Federal Student Aid's PRR Process Standards. In addition, if an IV&V vendor participated in the system component, the signature indicates that independent quality assurance activities were performed according to Federal Student Aid Standards and that the findings identified by IV&V are described in the presentation/supporting documentation.

Federal Student Aid's CIO - The Federal Student Aid CIO's signature certifies that all reasonable due diligence has been exercised to assure system stability and operability, and that risks identified and described in the presentation/supporting documentation are reasonable given the expected business benefit. The CIO's signature also certifies that the implementation of the system component or release is in alignment with Federal Student Aid's strategy for alignment of information technology investments, as required by the Clinger-Cohen Act.

Application Owner - The application owner's signature certifies acceptance of all business risks associated with implementation of the system or release. This specifically includes the risk of exposing the system or release to end users, including the public for certain releases.

SECTION 8. DELIVERABLES

The Technical Lead should retain the original, completed sign-off memorandum, along with detailed supporting documentation. A copy of the sign-off memorandum, PRR Presentation, completed PRR Checklist, and supporting documentation should be delivered to the project manager for the project, and another copy should be delivered to the CIO Enterprise Quality Assurance Team. The Enterprise Quality Assurance Team point of contact is Trey Wiesenburg.

Appendix A – Acronyms and Abbreviations

Appendix A - Acronyms and Abbreviations

ACS	Administrative Communications Systems
ATG	Assistive Technology Group
ATO	Authorization to Operate
C&A	Certification & Accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management
CMDB	Configuration Management Database
COO	Chief Operating Officer
COR	Contracting Officer Representative
COTS	Commercial-off-the-Shelf
CSO	Computer Security Officer
ED	Department of Education
EIT	Electronic and Information Technology
EOCM	Enterprise Operations Change Management
EQA	Enterprise Quality Assurance
FIPS	Federal Information Processing Standard
G.A.	Guarantee Agency
GAO	General Accounting Office
GPRA	Government Performance and Results Act of 1993
IATO	Interim Approval to Operate
IEEE	Institute of Electrical and Electronics Engineers
IPC	Investment Planning Council
IST	Inter-System Testing
IT	Information Technology
ITIM	Information Technology Investment Management
IV&V	Independent Verification & Validation
LCM	Life Cycle Management
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer

OMB	Office of Management & Budget
ORR	Operational Readiness Review
PIR	Post-Implementation Review
POC	Point of Contact
PRR	Production Readiness Review
QA	Quality Assurance
RACI	Responsibility, Accountability, Communication, Informed
SDR	Service Delivery Review
SLA	Service Level Agreement
SP	Special Publications
SRR	Security Readiness Review
SSO	System Security Officer
VDC	Virtual Data Center

Appendix B – Glossary

Appendix B - Glossary

Term	Definition
Business Function	A function that aligns with the mission of the agency (i.e., Loan Consolidation, Reconciliation, Auditing, Business Metric Management). (Definition Source: Created by the group in a meeting)
Common Infrastructure Service(s)	Information resources that provide functionality that is shared with other information resources that exist in multiple systems (i.e., Authentication and Authorization (SA), WebSphere Application Cluster Server, Oracle DBMS Clusters). (Definition Source: Created by the group in a meeting)
Information Resource	Information and related resources, such as personnel, equipment, funds and information technology (i.e., Oracle Financials 11i, WebSphere Application server, HP RP5400 Server, Cisco 2900 Series Routers, PIX 500 Series Firewalls). (Definition Source: FIPS 199 02/2004)
System (i.e., information system)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposal of information. (Definition Source: FIPS 199 02/2004)
System Component	A functional unit that publishes and/or processes information with an independent software code base that provides specific functionality for a system this is produced through a software development process or commercial-off-the-shelf (COTS) implementation. (Definition Source: Created by the group in a meeting)

Appendix C – Summary Checklist

Appendix C - Summary Checklist

Purpose: The purpose of this checklist is to provide a guideline for the items that are appropriate to support a PRR. This checklist may be tailored to the particular needs of each system/release. A final version of the checklist may indicate that a gap exists (e.g., user training was not completed); in such cases, the managers attending the PRR will make a decision about signing off on the PRR with a gap present. A gap in the checklist simply indicates a risk that needs to be considered prior to moving to production.

CRITERIA DESCRIPTION	GAP (Y/N)	COMMENTS/ HOW VALIDATED (Document Name)	POINT OF CONTACT	RISKS IDENTIFIED	PROPOSED RISK MITIGATION
Application/System Name:					
1. INVESTMENT INFORMATION					
1. Approved Business Case		[Business Case name or OMB control number]			
2. Contract or Task Order		[Contract Vehicle] [Contract number]			
3. Project Plan					
4. Project Schedule					
2. VIRTUAL DATA CENTER (VDC)					
1. Request for VDC Services Form (Service Management Request for VDC Services)		Capture Control Number:_____			
2. Operational RACI (Responsibility, Accountability, Communication, and Informed) completed					
3. Configuration Management Database (CMDB) Updates		CMDB information reviewed on [date]			

Application/System Name:					
CRITERIA DESCRIPTION	**GAP (Y/N)**	**COMMENTS/ HOW VALIDATED (Document Name)**	**POINT OF CONTACT**	**RISKS IDENTIFIED**	**PROPOSED RISK MITIGATION**
4. SDR Successfully Completed		SDR completed on [date]			
5. Change Requests Submitted (for production migration)		[VDC Change Request Number and Date submitted]			
6. Revalidate System Disaster Recovery Objectives, including both Recovery Time Objective (RTO) and Recovery Point Objective (RPO).		[System is **Mission Important**, RTO: 48 hours, RPO: 24 hours. or **Mission Supportive**, RTO: 72 hours, RPO: 48 hours.]			
3. SYSTEM SUPPORT PROCESSES					
1. Government Requirements Management Plan					
2. Requirements Traceability Matrix					
3. Configuration Management Plan					
4. Version Control Procedures					
5. Configuration Item Library					
6. Operational Change Control Procedures					

Application/System Name:

CRITERIA DESCRIPTION	GAP (Y/N)	COMMENTS/ HOW VALIDATED (Document Name)	POINT OF CONTACT	RISKS IDENTIFIED	PROPOSED RISK MITIGATION
4. TECHNICAL ARCHITECTURE					
1. Architecture Design					
2. Development (i.e. coding) Standards					
5. LICENSING					
1. Software License Requirements (including Paid Licenses)					
6. SECURITY					
1. Application Owner Identified		Name:			
2. System Security Officer Identified		Name:			
3. Revalidate System Categorization (High, Moderate or Low)		[Low / Moderate / High]			
4. Security Controls are identified in Security Plan and Assessed		[Yes/No/NA]			
5. Is C&A required?		[Yes/No]			
6. Human and Machine Readable Privacy Policy Completed		[Yes/No/NA]			
7. Privacy Impact Assessment review completed		[Yes/No/NA]			
8. Systems of Record review completed		[Yes/No/NA]			
9. Is the documentation of system configuration settings and hardening procedures completed?		[Yes/No/NA] [Reference document]			
10. Vulnerability Scans Completed? Have all findings from the scans been remidiated?		Date of last scan: Findings Remediated? [Yes/No]			

Application/System Name:

CRITERIA DESCRIPTION	GAP (Y/N)	COMMENTS/ HOW VALIDATED (Document Name)	POINT OF CONTACT	RISKS IDENTIFIED	PROPOSED RISK MITIGATION
7. TESTING					
1. Test Results Approval completed and signed to include client and user signoff of all testing results. Test Summary provided.		[Yes/No]			
2. Core LCM and Work Products Guide test documents delivered to include Test Readiness Review Checklists, Test Plan(s), Test Suites (Test Scripts/Test Cases).		[Yes/No] [Reference documents]			
3. Security Testing addressed if needed – Security Readiness Review (SRR).		[Yes/No/NA]			
4. Completed Accessibility Testing for compliance with Section 508 of the Rehabilitation Act.		[Yes/No/NA]			
5. Test Defects are tracked and mitigated (Defect Log). These defects are reported by test phase, severity and status.		[Yes/No/NA] [Test results reported in PRR by test phase, severity, and status – template provided]			
6. Number and severity of open defects documented and agreed to by Federal Student Aid management (example: No urgent, high or medium defects). Open defect responsibility identified and time to correct agreed upon.		[Test defects that have been accepted or deferred are documented in PRR Presentation.]			

Application/System Name:

CRITERIA DESCRIPTION	GAP (Y/N)	COMMENTS/ HOW VALIDATED (Document Name)	POINT OF CONTACT	RISKS IDENTIFIED	PROPOSED RISK MITIGATION
8. TRAINING					
1. Training Activities are completed and documented.		[Date completed, activities described in presentation]			
2. Call Center or Help Desk Script Updates are completed and documented.		[Date completed, updates described in presentation]			
9. SUPPORT STAGE					
1. Support available for Software Package					
2. VDC Service Desk Notified of Release					
3. Application Service Desk established					
4. Organizational Design and Skills Identified					
5. Maintenance and Operations Plan					
6. Post-Implementation Review (PIR) Advance Packet received					
7. Updated Lessons Learned Database for this release					

Appendix D – Checklist Definitions

Appendix D - Checklist Definitions

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
1. INVESTMENT INFORMATION	
1. Approved Business Case	**POC: Technical Lead / Project Manager / Project Sponsor** Business Case that was developed for the IT Investment and approved by FSA Management (OMB 300, Business Case, Project Concept Document, Business Case Light, etc).
2. Contract or Task Order	**POC: Technical Lead / Project Manager** Contract vehicle (ITSS BPA, EDSS, etc) to obtain required services or development effort and the specific contract number(s). Multiple contracts may be listed if there are multiple contracts needed to support the development (i.e. different contracts for requirements, design and development, O&M, etc).
3. Project Plan	**POC: Technical Lead / Project Manager** Project plan document.
4. Project Schedule	**POC: Technical Lead / Project Manager** Project schedule with start, end, and milestone dates.
2. VIRTUAL DATA CENTER (VDC)	**General POC:** **Federal Student Aid/CIO/IT Services** **Slawko Senaszczuk, VDC Manager** **Wanda Broadus, VDC Service Management** **Note: For applications/releases in the VDC, see the VDC Migration Checklist.**

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
1. Request for VDC Services Form (Service Management Request)	**POC: Technical Lead/VDC Manager** This form requests an overview of services and resources required from the VDC. Note that the Capture Control Number must be identified for this form and included on the checklist.
2. Operational RACI completed	**POC: Technical Lead/VDC Manager** This is a key component of the operational implementation and ensures that due diligence was performed by the VDC Team. Operational RACI stands for Responsibility, Accountability, Communication, and Informed. The RACI document is a matrix of the roles and responsibilities for all parties involved in the project (i.e. development contractor, data center contractor, other contractor teams, and federal staff). Many key activities are included under this activity including verification of responsibilities: (Primary Lead, Support Role, or Joint Responsibility), the requirements for the VDC environment have been communicated, all core LCM and Work Products Guide documents have been delivered including the SLAs, Implementation Plans, Maintenance and Operations Plan, Data Migration Plans, Data Management Plan, Configuration Management Plan, Disaster Recovery Plan, Security Plan, Business Continuity Plan, System Start-up Plan and the required accompanying procedures.
3. Configuration Management Database (CMDB) Updates	**POC: Technical Lead and VDC Manager** The CMDB should be updated. Completing the update the CMDB is required for the successful completion of the Service Delivery Review (SDR). The team should also review the Technical Support, Operations, Automation, and Communications required for the new system. The VDC environment needed by the system and estimated number of users should also be described. (Ref: VDC Configuration Management Database Data Dictionary, Version 1.0 (May 22, 2007))

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
4. Service Delivery Review (SDR) Successfully Completed	**POC: Technical Lead and VDC Manager** VDC review of operational support for the system in the production environment. This review ensures that the VDC can provide the resources needed to support the system in the production environment. The SDR is always completed prior to the Production Readiness Review (PRR).
5. Change Requests Submitted (for production migration)	**POC: Technical Lead and VDC Manager** Has the change request for the migration to the VDC Production environment been submitted?

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
6. Revalidate System Disaster Recovery Objectives, including both Recovery Time Objective (RTO) and Recovery Point Objective (RPO).	**POC: VDC Manager** For purposes of the PRR, please report the RTO and RPO that have been identified for the system in the disaster recovery plan, business continuity plan, or other appropriate documentation. RTO and RPO should be based on how the system is categorized for disaster recovery purposes (if the system is mission important or mission supportive). **Recovery Time Objective (RTO):** 1. The period of time within which systems, applications, or functions must be recovered after an outage 2. The maximum acceptable length of time that can elapse before the lack of a business function severely impacts the business entity. The RTO is comprised of two components: the time before a disaster is declared, and the time to perform tasks (documented in the Continuity of Services Plan) to the point of business resumption. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. RTO is sometimes referred to as Maximum Allowable Downtime (MAD). **Recovery Point Objective (RPO):** 1. The acceptable amount of lost data between the actual disaster last backup. **2.** The date and time of the last backup that data will be restored to. <table><tr><td>**VDC Standards**</td><td>Mission Important</td><td>Mission Supportive</td></tr><tr><td>RTO</td><td>48</td><td>72</td></tr><tr><td>RPO</td><td>24</td><td>48</td></tr></table>
3. SYSTEM SUPPORT PROCESSES	

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
1. Government Requirements Management Plan	**POC: Technical Lead** Plan that documents how the requirements process is managed.
2. Requirements Traceability Matrix	**POC: Technical Lead** Matrix that traces high-level requirements to detailed requirements then to specific test cases and the results of testing.
3. Configuration Management Plan	**POC: Technical Lead** Configuration Management (CM) is the process of identifying, organizing and managing the integrity of the project work products throughout the project's life cycle. Key Components include: Baseline Work Products, Mechanism to Track and Control Changes, Change Requests, and Mechanism to Establish and Maintain Baseline Integrity.
4. Version Control Procedures	**POC: Technical Lead** Procedures that describe how document and code versions will be managed.
5. Configuration Item Library	**POC: Technical Lead** A configuration item library is a repository for storing configuration items and their associated records. This library includes source code.
6. Operational Change Control Procedures	**POC: Technical Lead** Procedures to ensure system changes are coordinated and documented.
4. TECHNICAL ARCHITECTURE	
1. Architecture Design	**POC: Technical Lead** Description of the development, test, and production environments available in project documentation. This includes Software Architecture Document and other relevant documents as outlined in the Work Products Guide.
2. Development (i.e., coding) Standards	**POC: Technical Lead** Verification of appropriate coding standards used. References particular standards used.
5. LICENSING	

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
1. Software License Requirements	**POC: Federal Student Aid/CIO/IT Services (Kim Parker)** Licenses are in place and verification that licenses are current.
6. SECURITY	**General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)**
1. Application Owner Identified	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Validate that the Application Owner identified in the System Security Plan is correct.
2. System Security Officer (SSO) Identified	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Validate that the SSO identified in the System Security Plan is correct.
3. Revalidate System Categorization (High, Moderate, or Low)	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Perform an internal revalidation of the system categorization in accordance with FIPS 199. The Categorization results from a system criticality and sensitivity analysis based on FIPS 199. Review the categorization in the last system risk assessment and update as necessary.
4. Security Controls are identified in the System Security Plan and Assessed	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Review the System Security Plan to determine if appropriate baseline security controls and associated enhancements in accordance with NIST SP 800-53 Revision 2 have been adequately addressed. The System Security Plan should document the agreed-upon set of security controls including the organization's justification for any refinements or adjustments to the initial set of controls.

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
5. Is C&A required?	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** The SSO should assess the release to determine if it is a significant change to the system that requires recertification.
6. Human and Machine Readable Privacy Policy	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Verify that the privacy policy is P3P compliant if the release involves a new or modified web site.
7. Privacy Impact Assessment Review Completed	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Verify that a privacy impact assessment has been completed.
8. Systems of Record review completed	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Determine if the intended purpose and use of the system has been modified in conjunction with the release and a new or updated system of record notice should be published.
9. Documentation of system configuration settings and hardening procedures completed	**POC: Technical Lead/Project SSO** **General POC: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** Verify that system configuration settings created or modified as a result of the release are documented (usually in the System Security Plan or supporting documentation) and compliant with Federal Student Aid and NIST configuration settings and hardening procedures for the particular hardware and software/application platforms used.

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
10. Vulnerability Scans Completed? Have all findings from the scans been remidiated?	**POC - Vulnerability Scans: VDC Security (Rick Reyes or David Elliott)** **POC - Finding Remediation: Federal Student Aid/CIO/Security & Privacy (Bob Ingwalson, Federal Student Aid's CSO)** The VDC requires that all applications moving to production complete vulnerability scans prior to going live. This item requires coordination with VDC operations and should be scheduled well in advance of the production date so that there is sufficient time to remediate findings from the scans.
7. TESTING	
1. All Test Results Approval Completed and signed to include client and user signoff of all testing results. Test Summary provided.	**POC: Technical Lead** Test results completed and approved by Technical Lead and User Acceptance Testing participants. All results have been approved by Federal Student Aid and sign off approval granted. The results should be documented by phase of testing, severity and status. (See Federal Student Aid Enterprise Testing Standards Handbook)
2. Core LCM and Work Products Guide Test Documents Delivered and approved to include Test Readiness Review Checklists, Test Plan(s), Test Suites (Test Scripts/Test Cases).	**POC: Technical Lead** Approved testing plans and scripts that are consistent with requirements. All documents were delivered and approved by Federal Student Aid. (See Enterprise Testing Standards Handbook for Templates of Test Plans, Test Scripts, etc.)
3. Security Testing Addressed if needed. SRR performed as necessary.	**POC: Project SSO** Security Readiness Review (SRR) performed to provide analysis of need for security testing. Test the security control for the system – each system could have different tests. Minimum test: access controls using password strength and the controls to limit access by user type. An SRR may be provided where the developer provides a presentation to the SSO outlining all security impacts of the release. Any change to the existing system that impacts system requirements for access control and data security protection.
4. Completed Section 508 Accessibility Testing	**POC: ED/OCIO/ATG (Don Barret)** All applications being integrated into the ED operating environment; EdNet,

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
Section 508 requirements tested and verified by ED Assistive Technology Group (ATG) located in FOB-6. POC: Don Barret	Ed.gov, ConnectEd, VDC, and stand-alone desktops, must be tested for accessibility. Each product, application, and/or web page (software) is tested to determine how accessible the software's business functions are and to determine if it is accessible to the disabled using the assistive technology currently in use at the Department and how well the software meets the ED Requirements for Accessible Design and the Federal accessibility standard; Electronic and Information Technology Accessibility Standards, 36 CFR Part 1194. The ATG provides an acceptance report that should be available at the PRR.

What/when is tested: Pre-acquisition testing of COTS products to determine degree of accessibility BEFORE purchase, post-acquisition testing before integration, and for in-house developed software, interim testing during the build/test phases.

Testing is performed with the software sponsor, the developer, and the OCIO AT Team testers, including disabled testers present. Where remediation is found to be necessary, additional tests must be performed.

Any exemption justification must include an AT Accessibility Review Report of all products considered to meet the agency need.

See OCIO Directive; OCIO: 3:105 Procuring Electronic and Information Technology (EIT) In Conformance with Section 508 of the Rehabilitation Act of 1973, as amended, for guidance. |

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
5. Test Defects are tracked and mitigated (Defect Log). These defects are reported by test phase, severity, and status.	**POC: Technical Lead** Test results completed and approved by Technical Lead. All defects accounted for and disposition noted prior to PRR. The Test Summary brings together all pertinent information about the testing, including an assessment about how well the testing has been done, the number of incidents raised and outstanding, and, crucially, an assessment about the quality of the system. Also recorded for use in future project planning is details of what was done and how long it took. Approved test results based on plans and scripts that are consistent with requirements. (See Federal Student Aid Enterprise Testing Standards Handbook for templates)
6. Number and severity of open defects at PRR documented and agreed to by Federal Student Aid management. (Example: No urgent, high or medium defects.) Open defect responsibility identified and agreed upon.	**POC: Technical Lead** List of known risks agreed to be resolved during and after implementation. Please reference the Federal Student Aid Enterprise Testing Standards Handbook for the current priority and definition of test defect categories.
8. TRAINING	
1. Training Activities are completed and documented	**POC: Technical Lead** Plan documenting all training activities for the system release. User Training conducted or scheduled. Any new functionality for a new release that affects relevant system operation and written procedures, installation set-up, on-going training must be documented.
2. Call Center or Help Desk Script Updates are completed and documented	**POC: Technical Lead** Any new functionality for a new release that affects relevant scripts and accompanying written procedures must be updated and documented.
9. SUPPORT STAGE	

CRITERIA DESCRIPTION	Point of Contact (POC)/Definition
1. Support available for Software Package	**POC: Technical Lead** Maintenance support for the system in the production environment.
2. VDC Service Desk Notified of Release	**POC: Technical Lead and VDC Manager** VDC Service Desk has been notified of the release and has been provided information regarding support for the system release.
3. Application Service Desk Established	**POC: Technical Lead** Identify the service desk location and phone number to assist users with resolving system errors, issues, and concerns.
4. Organizational Design and Skills Identified	**POC: Technical Lead** List of specific and unique skills within Federal Student Aid necessary to maintain the system in the production environment.
5. Maintenance and Operations Plan	**POC: Technical Lead** Plan for transition of the system from the development and testing environments to the staging and production environments. Maintenance and Operations Plan should be delivered as outlined by the Work Products Guide.
6. Post-Implementation Review (PIR) Advance Packet received	**POC: Federal Student Aid/CIO/QA Team (Francis Tang)** The advance packet helps the project team prepare the PIR in advance after deployment of the project. The checklist for PIRs and the list of documents required to support PIRs are especially useful.
7. Update Lessons Learned Database	**POC: Federal Student Aid/CIO/QA Team (John Olumoya)** Use the CIO Quality Assurance Template to provide lessons learned for this release.

Appendix E – Sample Production Readiness Review Sign-Off Memo

Appendix E - Sample PRR Sign-Off Memo

PRR Sign-Off Memorandum

[Date]

This certifies that the [system/release name] has been appropriately tested and that all known risks have been disclosed. By signature below, Federal Student Aid accepts the risks associated with implementing this release into the production environment.

System Technical Lead: _____
                                {Name}

System Security Officer: _____
                                {Name}

Virtual Data Center Manager: _____
                                Slawko Semaszczuk or designee

Enterprise Quality Assurance   _____
                                Mike Rockis or designee

Federal Student Aid's CIO: _____
                                John Fare or designee

Application Owner: _____
                                {Name}

Sign-off Type: ❑ Unconditional   ❑ Conditional   ❑ Provisional   ❑ No Sign-off

Appendix F - References

Appendix F - References

This Process Description was created in accordance with the following Federal Student Aid policies:

- Clinger-Cohen Act of 1996, P.L. 104-106

- Department of Education, Department Directive OCIO: 3-105, *Procuring Electronic and Information Technology (EIT) In Conformance with Section 508 of the Rehabilitation Act of 1973,* dated 05/01/2006

- Department of Education, Department Directive OCIO: 3-108, *Information Technology Investment Management (ITIM) and Software Acquisition Policy,* dated 9/15/2006

- Department of Education, Department Directive OCIO: 1-106, *Lifecycle Management (LCM) Framework,* dated 12/2/2005

- Department of Education, Federal Student Aid, *Work Products Guide*, Version 4.0, dated 9/17/2007

- Department of Education, Federal Student Aid, Enterprise Operational Change Management Plan, Version 1.1 (November 7, 2007)

- Department of Education, Federal Student Aid, *Enterprise Testing Standards Handbook,* Version 1.0, dated September 30, 2007

- Department of Education, Federal Student Aid, *Independent Verification & Validation Handbook,* Version 3.0, dated February 15, 2006

- Department of Education, Federal Student Aid, *Virtual Data Center Configuration Management Database Data Dictionary,* Version 1.1 (November 7, 2007)

- Federal Information Processing Standards (FIPS) 199 – *Standards for Security Categorization of Federal Information and Information Systems*

- Government Performance and Results Act of 1993, P.L. 103-62

- National Institute of Standards and Technology, Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*

- National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* dated May 2004

- National Institute of Standards and Technology, Special Publication 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems,* dated December 2007

- OMB Circular A-11 – *Preparation, Submission, and Execution of the Budget, Capital Asset Plan and Business Case*

- OMB Circular A-130 – *Management of Federal Automated Information Resources*

Appendix G – PRR Slide Template

Appendix G – PRR SLIDE TEMPLATE

Agenda

1. Business Background
2. Schedule
3. Testing Summary
4. Collaboration and Coordination
5. IV&V Recommendation
6. Risk Summary
7. Lessons Learned
8. Meeting Closure

2

START HERE
GO FURTHER
FEDERAL STUDENT AID

Background
Business Drivers

- [list business drivers, including legislation, increased functionality, etc.]

3

START HERE
GO FURTHER
FEDERAL STUDENT AID

Background
Business Benefits

- [list anticipated business benefits from the release, such as cost savings, more efficient processing, etc.]

4

START HERE
GO FURTHER
FEDERAL STUDENT AID

Schedule
High-Level Milestones

	Planned (baseline) Completion	Actual Completion
Requirements	1/30/2008	2/30/2008
Design	2/30/2008	4/20/2008
Development	5/30/2008	7/30/2008
Integration Testing	6/10/2008	8/10/2008
System Testing	6/15/2008	8/15/2008
Intersystem Testing	6/30/2008	8/30/2008
User Acceptance Testing	7/30/2008	9/30/2008
508 Compliance Testing	8/5/2008	10/5/2008
Performance Testing	8/10/2008	10/10/2008
SDR	8/15/2008	10/15/2008
PRR	8/30/2008	10/30/2008
Production Cutover	9/1/2008	11/1/2008

Complete project schedule is available from
Jane Doe, jane.doe@ed.gov.

[Note: Milestones listed on this slide should be tailored to fit the project]

START HERE
GO FURTHER
FEDERAL STUDENT AID

5

Testing Summary

TEST PHASE	High Level Summary of Test Results
Integration Testing – Jointly executed by xxx team. Focused on how two or more components worked together.	▪Configuration Management Problems ▪Unable to rely on testing results
System Testing – Jointly executed by xxx and xxx teams. Focused on how two or more components worked together.	▪Configuration Management Problems ▪Unable to rely on testing results
Inter-system Testing ("end-to-end" testing) – Performed by the xx team in conjunction with external entities (e.g., SSA, IRS) and internal entities (e.g., NSLDS, COD). Purpose is to test data flows and functionality between multiple systems.	▪Team considers the IST to be a success
User Acceptance Testing – Performed by XX and YY teams. Focused on validating that major business processes work as expected.	▪Configuration Management Problems ▪Unable to rely on testing results ▪xxx prevented successful completion
508 Compliance testing - The 508 testing was conducted by the contractor and by the Chief Information Officer (CIO). The purpose of 508 testing is to verify system components meet Department of Education 508 compliance standards.	▪Sample testing of forms was completed ▪93.7% of the 333 XX forms are compliant ▪Users of the 21 non-compliant forms can be accommodated.
Performance testing – Production processing times were compared to the test environment.	▪Capacity performance problems found and requested more servers to handle capacity

[Note: Please address each of the test phases included above.]

START HERE
GO FURTHER
FEDERAL STUDENT AID

6

[Note: It is preferred that test results be reported in the format below.]

Summary of Test Results

Incident Report By Testing Phase

Type of Testing	OPENED					CLOSED					DEFERRED					ENHANCEMENTS				
Priority	Urgent	High	Med	Low	Total	Urgent	High	Med	Low	Total	Urgent	Hgh	Med	Low	Total	Urgent	Hgh	Med	Low	Total
Integration	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
System	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
Intersystem	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
User Acceptance	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
508 Testing	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
Performance	4	4	4	4	16	1	1	1	1	4	1	1	1	1	4	2	2	2	2	8
TOTALS	24	24	24	24	96	6	6	6	6	24	6	6	6	6	24	12	12	12	12	48

Urgent – issues currently in production that must be addressed immediately
High – highest significance, showstoppers, errors related to incorrect data,
Med – mid level, do not impact timely completion of implementation, a workaround can be used;
Low – issues that, if not resolved, will not impact business operations

[See: Enterprise Testing Standards Handbook for elaboration on categories. The categories listed above are the FSA standard categories for reporting test results. If a system has not adopted these standard categories, this slide may be tailored to fit the categories used by the system.]

START HERE
GO FURTHER
FEDERAL STUDENT AID

7

Collaboration and Coordination
Security Reviews

- System is classified as a Minor Application
- System is FIPS 199 Security Categorization "Low"
- Confidentiality, Integrity, and Availability are all categorized as "Low"
- The following documents are complete:
  - CIP Survey (date completed/updated)
  - Privacy impact assessment (date completed/updated)
  - Self-Assessment (date completed/updated)
  - System Security Plan (date completed/updated)
  - Inventory Worksheet (date completed/updated)
- CIO successfully performed vulnerability scans on 5/15
- ISSO is Jane Doe, confirmed by assignment memo dated 5/1/2008

8

START HERE
GO FURTHER
FEDERAL STUDENT AID

Collaboration and Coordination
Disaster Recovery and Business Continuity

- VDC has been notified of system disaster recovery and business continuity needs.
- Recovery Time Objective (RTO): [Mission Important = 48 hours or Mission Supportive = 72 hours]
- Recovery Point Objective (RPO): [Mission Important = 24 hours or Mission Supportive = 48 hours]

9

START HERE
GO FURTHER
FEDERAL STUDENT AID

Collaboration and Coordination
Data Center Readiness

- CMDB review and validation occurred on 5/15/2008
- Perot Systems conducted a Service Delivery Review (SDR) on 5/16/2008
- There were no outstanding issues from the SDR [or report outstanding issues from SDR].
- Perot indicated closeout of SDR via e-mail on 5/20/2008

10

START HERE
GO FURTHER
FEDERAL STUDENT AID

Collaboration and Coordination
Applications Maintenance Readiness

- All required documentation is complete [or report outstanding documentation]
- XYZ is contracted for ongoing content updates
- ABC will perform O&M activities

11

START HERE
GO FURTHER
FEDERAL STUDENT AID

Collaboration and Coordination
Help Desk Readiness

- Service Desk and/or call center is ready to receive calls
- Number is 1-800-XXX-XXXX
- VDC Service Desk has been notified of release
- Call volume will be included in weekly status reports and Federal Staff will perform random monitoring of calls

12

START HERE
GO FURTHER
FEDERAL STUDENT AID

Independent Verification & Validation (IV&V)

- IV&V recommendation

  [Note: Coordinate with IV&V lead to determine how IV&V will present at PRR. For larger projects, IV&V may provide an entire presentation of their own for PRR, for smaller efforts IV&V may be included as part of this presentation.

  Some projects may not use IV&V at all and this slide may be omitted or marked "N/A" in those cases.]

13

START HERE
GO FURTHER
FEDERAL STUDENT AID

Risk Summary

- Risk: Insufficient Memory
- Mitigation: More memory added on [date]
- Probability: Low
- Impact: Moderate

14

START HERE
GO FURTHER
FEDERAL STUDENT AID

Risk Summary

- Risk: Unpredictable volume putting increased load on site
- Mitigation: Release 1.0 will be a static site largely served by Akamai. This risk is also mitigated by the fact that this is a 'beta' launch and not being actively publicized through an outreach program
- Probability: Low – with Akamai in place
- Impact: There should be no impact with the site being served through Akamai

15

START HERE
GO FURTHER
FEDERAL STUDENT AID

Risk Summary
Outstanding Issues/Action Items

- No outstanding (unmitigated) issues for this release
- Action items include upgrading memory after the system has gone to production

16

START HERE
GO FURTHER
FEDERAL STUDENT AID

Lessons Learned

- A cross-functional, cohesive management team is essential to proper project tracking:
  - A single point of contact in contracts helps eliminate / limit schedule delays
  - A cross-functional management team enables a more cohesive and strategic acquisition strategy that is essential for future success
- Having 508 compliance staff involved at the beginning was beneficial
- Having weekly CIO touch point meetings kept everyone informed and eliminated some uncertainties

17

START HERE
GO FURTHER
FEDERAL STUDENT AID

Meeting Closure

- Seeking unconditional sign-off
- Completion of formal sign-off memorandum
- Delivery of sign-off memorandum and supporting documentation to CIO/Enterprise Quality Assurance Team

18

START HERE
GO FURTHER
FEDERAL STUDENT AID